



FIRMWARE ANALYSIS AND COMPARISON TOOL

Firmware Analysis of Cisco/Linksys SRW2008 - 1.0.4

Meta Data

HID	Cisco/Linksys SRW2008 - 1.0.4
Device Name	SRW2008
Vendor	Cisco/Linksys
Device Class	Switch (Managed)
Version	1.0.4
Release Date	2007-09-06
Size	3.22 MiB (3,378,139 bytes)

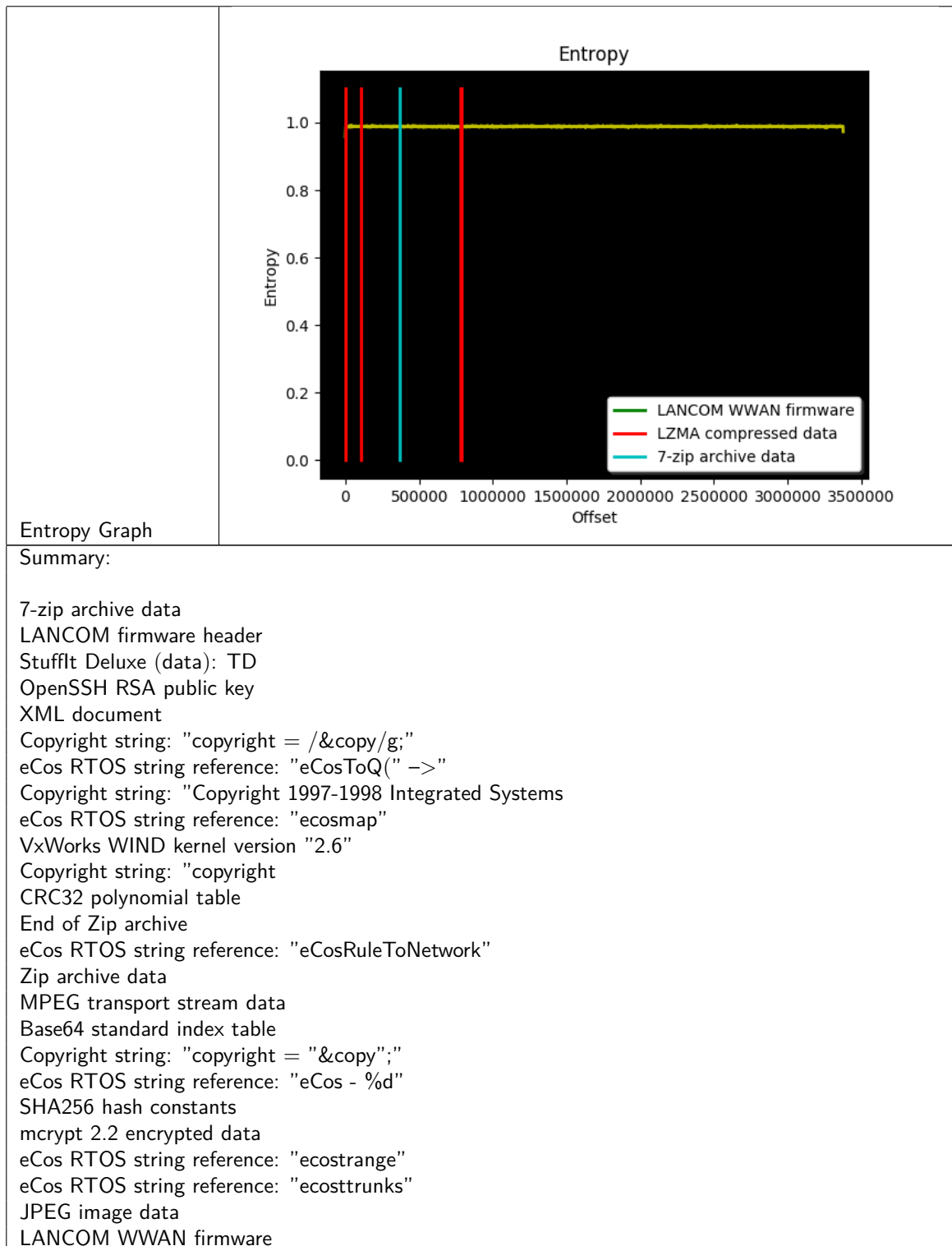
Analysis

base64decoder

Time of Analysis	2018-03-29 12:54:45
Plugin Version	0.1.2
Summary	Base64 code detected

binwalk

Time of Analysis	2018-03-29 12:57:40
Plugin Version	0.5
Signature Analysis:	
DECIMAL HEXADECIMAL DESCRIPTION	
<hr/>	
81 0x51 LANCOM WWAN firmware	
272 0x110 LZMA compressed data, properties: 0x5D, dictionary size: 8388608 bytes, uncompressed size: 550208 bytes	
105822 0x19D5E LZMA compressed data, properties: 0x5D, dictionary size: 8388608 bytes, uncompressed size: 1049671 bytes	
368135 0x59E07 7-zip archive data, version 0.2	
781528 0xBECD8 LZMA compressed data, properties: 0x5D, dictionary size: 8388608 bytes, uncompressed size: 27900 bytes	
790127 0xC0E6F LZMA compressed data, properties: 0x5D, dictionary size: 8388608 bytes, uncompressed size: 9596576 bytes	



PARity archive data - file number 1
 GIF image data
 Ubiquiti firmware header
 LZMA compressed data
 Certificate in DER format (x509 v3)
 Copyright string: "Copyright 1986-1997 Epilogue Technology Corporation"
 HTML document footer
 eCos RTOS string reference: "eCost"
 Copyright string: "Copyright 1984-2002 Wind River Systems"
 Neighborly text
 HTML document header
 eCos RTOS string reference: "eCosToQ(COSNum)"
 OpenSSH DSA public key
 VxWorks operating system version "5.5.1"

cpu architecture

Time of Analysis	2018-03-29 12:57:52
Plugin Version	0.3.1

crypto material

Time of Analysis	2018-03-29 12:57:41
Plugin Version	0.5

exploit mitigations

Time of Analysis	2018-03-29 12:57:54
Plugin Version	0.1.1

file hashes

Time of Analysis	2018-03-29 12:58:01
Plugin Version	1.0
imphash	None
md5	9665a7ad243bda91ce6312ed3aab305d
ripemd160	5e0313f309e610bece33bfece02a933bb80bc7b9
sha1	5ea563d79a7ed3f8c7a872e0bf31db9ef8c90711
sha256	b7c55a6de9fd1b85ec07f661b4d21638021999e2b1e754de1922f3b01f2cedb8
sha512	937f575dfffce1f986faf4ca8e3ba836f6d6f9dfaab582c4561fa93c7c2b 0ceee92efdb3e3e87abe0bbf9a867bd3f1169f27c06e7f467f549b0d40c3f814217
ssdeep	98304:nNasK108t/KzpM7NURKVt9RMN6sc0KzLgP:nNFK1Dt/KFMX0670KIP
whirpool	69477a040d3430dc6706d1bb6a4e2088814e24e6f3d73eb14b2e0e41aee6b a0220d98a4896b872abd558c9cd4945c7861e76fca8e6846f650940482c7697ce48

file type

Time of Analysis	2018-03-29 12:57:50
Plugin Version	1.0
File Type	ROS Container
MIME	firmware/ros
Summary	application/x-lzma firmware/ros application/x-java-applet application/x-7z-compressed text/plain image/gif application/octet-stream application/zip image/jpeg

init systems

Time of Analysis	2018-03-29 12:57:58
Plugin Version	0.4.1

ip and uri finder

Time of Analysis	2018-03-29 12:57:48
Plugin Version	0.4.1
IPs v4	1.0.4.1
IPs v6	:: 0:: 3:: ::c ::D 5:: ::7 ::6B ::4 B:: E:: ::9a9 A:: b::
URIs	list is empty
Summary:	1.1.1.10 b:: 224.0.0.255

7.2.1.16
1.6.1.1
tftp://oob/10.1.2.3/saved-image-file
7.2.1.10
4.1.89.98
1.1.1.6
64.4.1.11
flash://image
http://www.linksys.com/
tftp://oob/10.7.8.9/my_boot.rfb
tftp://oob/10.4.5.6/my_image.dos
tftp://10.0.0.9/commands-file
0.0.0.255
10.1.1.3
7.10.1.4
2.1.16.1
64.4.1.10
3::
0.0.255.255
::4
1.89.64.5
E::
1.89.98.2
0::
10.1.2.3
224.0.0.251
2.1.31.1
64.4.1.8
64.5.1.5
1.1.1.15
2.1.10.7
1.1.1.14
aposhttp://mynsURI
64.5.1.6
1.1.1.9
10.0.0.9
1.1.1.12
1.0.4.1
10.1.2.2
7.2.1.4
::1
64.4.1.5
tftp://10.1.2.3/saved-config
unit://member/filename
tftp://10.0.0.2/saved_cfg
unit://3/image
1.1.1.8
tftp://oob/ip

239.255.255.250
1.1.1.11
64.4.1.2
4.1.89.64
192.168.1.254
1.1.1.2
89.98.2.1
0.255.0.0
<http://www.w3.org/1999/XSL/Transform>
255.255.255.255
::
64.4.1.9
171.205.239.111
64.5.1.1
10.0.0.2
10.0.0.6
tftp://ip
::7
<http://www.linksys.com>
7.10.1.3
tftp://10.4.5.6/my_image.dos
1.0.0.0
7.2.1.8
1.3.3.1
255.255.255.0
tftp://10.1.2.3/my_image.ros
5::
1.1.1.7
1.1.1.3
7.2.1.9
9::9996
10.1.2.1
64.4.1.3
64.4.1.6
2.2.1.17
1.1.1.16
tftp://10.0.0.6/saved-boot-image
255.255.0.255
flash://filename
224.0.0.0
1.89.64.4
7.2.1.3
10.7.10.1
149.36.184.198
0.0.0.0
unit://4/boot
2.2.1.1
1.1.1.18

2.2.1.16
64.4.1.4
1.1.1.5
64.4.1.1
2.2.1.10
::6B
239.255.255.255
1.1.1.17
B::
tftp://10.1.2.3/my_boot.rfb
::FFFF
tftp://10.1.2.3/my_image.dos
64.4.1.7
<http://www.w3.org/1999/xhtml>
176.212.0.0
10.7.8.9
flash://startup-config
0.0.255.0
10.1.1.2
3.6.2.4
unit://2/image
1.1.1.13
::9a9
tftp://oob/10.1.2.3/saved-config
0.9.6.1
64.5.1.2
64.5.1.3
::c
255.0.0.0
64.4.1.12
2.2.1.11
A::
1.1.1.19
::D
10.1.1.1
0.255.255.255
6.3.10.1
7.2.1.13
tftp://10.7.8.9/my_boot.rfb
1.1.1.4
tftp://10.1.2.3/saved-image-file
e::
tftp://oob/
tftp://10.0.0.6/saved-image
255.0.255.255
10.4.5.6
127.0.0.1
<http://www.openssl.org/support/faq.html>

software components

Time of Analysis	2018-03-29 12:57:44
Plugin Version	0.3
Summary	VxWorks 5.5.1 OpenSSL OpenSSL 0.9.8 GoAhead OpenSSH

printable strings

Time of Analysis	2018-03-29 12:57:47
Plugin Version	0.2
String Count	7262

users and passwords

Time of Analysis	2018-03-29 12:54:43
Plugin Version	0.4

string evaluator

Time of Analysis	2018-03-29 12:57:57
Plugin Version	0.2
String Count	7262

unpacker

Time of Analysis	2018-03-29 12:54:36
Plugin Version	0.7
Plugin	ROSTFile
Extracted	6
Output:	

ROS PACK firmware archive payload extractor

Version 0.6

(c) Copyright 2015 TJ <hacker@iam.tj>

Licensed on the terms of the GNU General Public License version 2

Filename: /media/data/fact_fw_data/b7/b7c55a6de9fd1b85ec07f661b4d21638021999e2b1e754de1922f3b01f2cedb8.3378139

File length: 3378139 (0x338bdb)

ARC Magic: LSS2

ARC Index: 1.01

Header version: 1

length: 48

Payload

length: 3378091 (0x338bab)

checksum: 430634778 (0x19aaf71a)

Link Time: 09:12:58

Link Date: 2007-09-06

Signature: PACK

Dir Entries: 6

Extracted CLI_FILE from offset 272 (105518 bytes)

Extracted DELSCRIF from offset 105822 (262313 bytes)

Extracted EWS_FILE from offset 368135 (413361 bytes)

Extracted UPNP_FILE from offset 781528 (8407 bytes)

Extracted DATETIME_C from offset 789935 (160 bytes)

Extracted RSCODE from offset 790127 (2588012 bytes)

Payload length: 3378091 (0x338bab)

Payload extracted: 3378091 (0x338bab)

Payload checksum: 430634778 (0x19aaf71a)

Calculated checksum: 430634778 (0x19aaf71a)

Size Packed -> Un-packed	3.22 MiB -> 3.22 MiB
Entropy	0.90
Summary	no data lost data lost unpacked

malware scanner

Time of Analysis	2018-03-29 12:54:40
Plugin Version	0.3
MD5	9665a7ad243bda91ce6312ed3aab305d
System Version	0.2.6
Scanners Number	1
Positives	0

Scanners	ClamAV
Scanns	ClamAV :: detected:False ClamAV :: result:clean ClamAV :: version:ClamAV 0.99.4/24430/Thu Mar 29 06:23:16 2018